MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102
Telephone: (702) 851-2180
Facsimile: (702) 851-2189
Email: *mbourassa@blgwins.com*
jfornetti@blgwins.com
vgray@blgwins.com

NICHOLAS A. COLELLA (*pro hac vice*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Email: *nickc@lcllp.com*

Counsel for Plaintiff Tausinga

Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA
***

IN RE HANKINS PLASTIC SURGERY ASSOCIATES, P.C. dba HANKINS & SOHN PLASTIC SURGERY ASSOCIATES This Document Relates to: All Actions	Master file No. 2:23-cv-00824-RFB-DJA **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jennifer Tausinga, Alysia Wrenn, and Olga Romashova (collectively, "Plaintiffs"), bring this Consolidated Amended Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant Hankins Plastic Surgery Associates P.C. dba Hankins & Sohn Plastic Surgery Associates ("Hankins" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge:

NATURE OF THE ACTION

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Hankins is a healthcare provider with locations in Henderson and Las Vegas, Nevada. Hankins provides plastic surgery care to patients across the greater Las Vegas Valley.[1]

4. As a healthcare provider, Hankins knowingly obtains, collects, and stores patient PII and PHI. In turn, Hankins has a resulting duty to secure, maintain, protect, and safeguard the PII and PHI that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. Despite Hankins' duty to safeguard its patients' PII and PHI, Plaintiffs' and other patients' PII and/or PHI was exfiltrated by a threat actor during a data breach of Defendant's computer network which occurred on or around February 23, 2023 (the "Data Breach").[2]

6. On or about March 14, 2023, Hankins began notifying affected patients and/or prospective patients, including Plaintiffs of "a recent data security event that may impact some of your

---

[1] *Hankins Plastic Surgery Center*, https://www.hankinsplasticsurgery.com/ (last visited Sept. 15, 2023).
[2] *Notice of Security Incident/Data Breach*, Hankins & Sohn Plastic Surgery Associates (Apr. 3, 2023), https://ago.vermont.gov/sites/ago/files/2023-04/2023-04-

information. We are providing you with information about the event, our response, and steps you can take to better protect your information against the possibility of misuse of your information, should you feel it appropriate to do so. We recently became aware of allegations by an unknown actor that data was stolen from our network. We are working diligently to assess these allegations and to confirm the nature and scope of the activity. We are also actively working with law enforcement to investigate the activity. We are reviewing the information that we store on our systems to identify current and former patients whose information may have been impacted by this event. …" A copy of one of these emails is attached as **Exhibit "1."**

7. When notifying its patients of the Data Breach, Hankins further warned that the threat actor intended to misuse the exfiltrated patient PII and PHI to commit extortion, informing patients that the threat actor "threatened to reach out to our patients individually." *See* **Exhibit "1."**

8. Based on the public statements of Hankins to date, a wide variety of patient PII and PHI was implicated in the Data Breach, including but not limited to patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical history, consultation notes, and photos.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII and/or PHI. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII and/or PHI; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to monitor and timely detect the Data Breach.

10. As a result of Defendant's failure to implement and follow basic data security procedures, Plaintiffs' and Class Members' PII and PHI is now in the hands of cybercriminals who wish to use it for nefarious purposes.

03%20Hankins%20%26%20Sohn%20Plastic%20Surgery%20Associates%20Data%20Breach%20Notice%20to%20Consumers.pdf ("Notice of Data Breach").

11. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risks which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

12. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for negligence, breach of implied contract, unjust enrichment, breach of confidence, violations of the Nevada Consumer Fraud Act, negligent misrepresentation, and seek to compel Defendant to adopt reasonably sufficient security practices to safeguard patient PII and PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future and to further provide Plaintiffs and Class Members with credit monitoring services for the rest of their lives.

PARTIES

13. Plaintiff Jennifer Tausinga is and, at all relevant times hereto, an adult who is a citizen and resident of the state of Nevada.

14. Plaintiff Tausinga is a patient of Hankins. On or about March 14, 2023, Plaintiff Tausinga received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

15. Plaintiff Alysia Wren is and, at all relevant times hereto, an adult who is a citizen and resident of the state of Nevada.

16. Plaintiff Wrenn is a patient of Hankins. On or about March 14, 2023, Plaintiff Wrenn received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

17. Plaintiff Olga Romashova is and, at all relevant times hereto, an adult who is a citizen and resident of the state of Nevada.

18. Plaintiff Romashova is a patient of Hankins. On or about March 14, 2023, Plaintiff Romashova received a notification from Defendant indicating that her PII and/or PHI may have been affected by the Data Breach.

19. Defendant Hankins is, and at all relevant times hereto, a Nevada professional corporation with a principal place of business located in Las Vegas, Nevada. Defendant Hankins is a citizen of Nevada.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

21. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

22. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

Hankins Collected and Stored Plaintiffs' and Class Members' PII and PHI.

23. Hankins is a plastic surgery group practice that provides the greater Las Vegas Valley "with the very best of surgical and nonsurgical care," including face, breast, body, and male plastic surgery along with non-surgical treatments including injectables and dermal fillers, skin resurfacing, skin tightening, laser hair removal, non-surgical body contouring, and skin care products.[3]

24. "At Hankins & Sohn Plastic Surgery Associates, our board certified plastic surgeons, W. Tracy Hankins, MD and Samuel M. Sohn, MD believe in patient safety, world-class results, and compassionate care. With this commitment in mind, we invite patients from around the world to experience the art and science of plastic surgery through the hands, hearts, and minds of Dr. Hankins and Dr. Sohn."[4]

25. As a condition of providing the above-described healthcare services to Plaintiffs and Class Members, Plaintiffs are informed and believe, that Hankins receives, creates, and handles PII and

---

[3] *Hankins Plastic Surgery Center*, https://www.hankinsplasticsurgery.com/ (last visited Sept. 15, 2023).
[4] *About the Practice*, Hankins Plastic Surgery Center, https://www.hankinsplasticsurgery.com/about/ (last visited Sept. 15, 2023).

PHI, which includes patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical histories, consultation notes, and photos.

26. Plaintiffs and Class Members must entrust Hankins with their sensitive and confidential PII and PHI in order to receive healthcare services, and in return reasonably expected that Hankins would safeguard their highly sensitive information and keep it confidential.

27. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII and PHI, Hankins assumed equitable and legal duties to safeguard and keep confidential Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

28. Even though "[t]he confidentiality, privacy, and security of information in [Defendant's] care are [its] highest priorities,"[5] Hankins nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and the exfiltration of Plaintiffs' and Class Members' PII and PHI stored within its computer network.

Hankins Breached its Duty to Protect its Patients.

29. Hankins was well aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

30. Hankins also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

31. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

32. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6] PHI, in addition to

---

[5] Notice of Data Breach, *supra* note 2.

[6] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

33. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[7]

34. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[8]

35. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[9] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[10]

36. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[11]

---

[7] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[8] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Sept. 15, 2023).

[9] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Sept. 15, 2023).

[10] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in %20victims'%20names.

[11] *Id.*

37. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[12]

38. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[13]

39. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

40. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

41. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Hanins's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

42. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's

---

[12] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 15, 2023).

[13] *Id.*

[14] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Sept. 15, 2023).

relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

43. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

44. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

45. **Driver's License Numbers—**are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive. This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, places of employment, doctor's offices, government agencies, and other entities.

---

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

46. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

47. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

48. **Medical Information**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[18]

49. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[19]

50. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of

---

[16] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[17] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[18] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Sept. 15, 2023).

healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[20]

51. According to Experian:

Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

Victims of healthcare data breaches may also find themselves being denied care, coverage, or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[21]

52. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

---

[19] Alder, *supra* note 10.

[20] *Id.*

[21] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[22] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 15, 2023).

53. Based on the value of its patients' PII and PHI to cybercriminals, Hankins knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. Hankins failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

Hankins Breached its Duty to Protect Patient PII and PHI.

54. On or about March 14, 2023, Plaintiffs received email notifications from Defendant, informing them that a threat actor had stolen data from Hankin's computer network. The email notice further informed Plaintiffs that the threat actor threatened to reach out to Defendant's patients about the stolen information, *i.e.*, the threat actor threatened to use the stolen information to extort Plaintiffs and other of Defendant's patients.

55. Despite the threat actor stealing information from Defendant's computer network and threatening to extort it patients, Defendant did not offer Plaintiffs or Class members identity theft protection services in its March 14,2023 email notice. Instead, Defendant simply advised Plaintiffs and class members to "lock down" their social media profiles and monitor their accounts.

56. On or about April 3, 2023, Defendant began mailing data breach notifications to impacted patients.

57. According to Hankins, on or about February 23, 2023, Defendant discovered suspicious activity relating to allegations made by a threat actor that data was stolen from its network.

58. Upon discovering the suspicious activity, Hankins investigated the claims of the threat actor and claims to have determined the nature and scope of the activity and what information was compromised. Hankins' investigation revealed that at some point prior to February 23, 2023, the threat actor had exfiltrated certain files from Hankins' computer network.

59. A wide variety of patient PII and PHI was compromised during the data breach, including but not limited to patient names, contact information, dates of birth, Social Security Numbers, driver's license information, medical histories, consultation notes, and photos.

60. Upon information and belief, following the Data Breach, the threat actor held the stolen information for ransom and demanded that Hankins pay. After Hankins refused to pay the ransom, the threat actor then began demanding ransom payments from individual patients. The threat actor warned

patients that if they refused to pay the ransom, the threat actor would send patients' stolen PII and PHI to their friends, families, and colleagues.

61. Following the threat actor's individual ransom attempts directed at Defendant's patients, the threat actor published the stolen information on its leak site(s). On the leak site(s), the threat actor claimed to have downloaded everything from Defendant's plastic surgery clinic's network, including documents and pre- and post-op photos pertaining to more than 10,000 of Defendant's patients. The stolen patient information posted on the leak site(s) includes 131 patients' nude photos, names, email addresses, and phone numbers.[23] The number of patients included on the leak site(s) appears to increase as time goes on.

62. The threat actor further advertised that patients could have their information removed from the leak site if they provided a review about Hankins. However, the threat actor made clear that they would not delete any of the stolen information and the leak site—the threat actor would only delete the website and stolen patient information if and when Hankins paid a ransom.

63. According to information provided to the Indiana Attorney General, the Data Breach impacted more than 12,000 individuals.[24]

64. Plaintiffs are informed and believe that the Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

FTC Guidelines Prohibit Hankins from Engaging in Unfair or Deceptive Acts or Practices.

65. Hankins is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act

---

[23] Due to the sensitive nature of the information displayed on the leak site, Plaintiffs have not provided a link to the leak site out of respect for individuals' privacy.

[24] *2023 Data Breach Year to Date Report*, Office of the Indiana Attorney General https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/2023-Data-Breach-Year-to-Date-Report.pdf (last visited Sept. 15, 2023).

66. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

67. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[26]

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Upon information and belief Hankins failed to properly implement one or more of the basic data security practices recommended by the FTC. Hankins' failure to employ reasonable and appropriate data security measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

71. Hankins was at all times fully aware of its obligations to protect the PII and/or PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of PII and/or PHI. Hankins was also aware of the significant repercussions that would result from its failure to do so.

---

[25] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Sept. 15, 2023).

[26] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Sept. 15, 2023).

[27] *Id.*

Hankins is Obligated Under HIPAA to Safeguard Patient PHI.

72. Hankins is required by the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*. to safeguard patient PHI.

73. Hankins is an entity covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI.

74. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

75. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

76. Under C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

77. HIPAA requires Hankins to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et seq*.

78. The Department of Health and Human Services Office for Civil Rights further recommends the following data security measures a regulated entity such as Hankins should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[28]

79. Upon information and belief, Hankins failed to implement one or more of the recommended data security measures.

80. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals, nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

81. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that they acquire, receive, and collect, and Defendant is further

[28] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dept't of Health & Human Services (mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

82. Given the application of HIPAA to Hankins, and that Plaintiffs and Class Members directly or indirectly entrusted their PHI to Defendant in order to receive healthcare services from Hankins, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

Plaintiffs' Experiences.

Plaintiff Tausinga

83. Plaintiff Tausinga was a patient of Defendant. On or about March 14, 2023, Plaintiff Tausinga received an email notification from Defendant informing her that the PII and PHI she provided to Hankins was compromised in the Data Breach.

84. Since the announcement of the Data Breach, Plaintiff Tausinga has experienced fraud. By March 28, 2023, the threat actor was threatening Plaintiff Tausinga through the WhatsApp mobile application to distribute her PII and PHI to her friends, colleagues, and neighbors, unless she paid a ransom to the threat actor directly. Plaintiff Tausinga later notified Hankins of the communication she received from the threat actor.

85. When Plaintiff Tausinga refused to pay the threat actor's demands, the threat actor shared her consultation photos with friends, colleagues, and neighbors. Hankins took no steps to prevent the release of the PII and/or PHI to Plaintiff Tausinga's friends, colleagues, and neighbors. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Tausinga has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to her friends, colleagues, and neighbors.

86. Since the announcement of the Data Breach, Plaintiff Tausinga has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Tausinga would not have to undergo such time-consuming efforts but for the Data Breach.

87. As a direct and proximate result of the Data Breach, Plaintiff Tausinga has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive

nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally used by the threat actor after the Data Breach to extort Plaintiff Tausinga.

Plaintiff Wrenn

88. Plaintiff Wrenn was a patient of Defendant. On or about March 24, 2023, photographs and information possessed and stored by Defendant, including images of Plaintiff Wrenn's medical treatment and of her medical charts, were made public via e-mails sent to Plaintiff Wrenn's employer and others.

89. Since the announcement of the Data Breach, and as recently as September 2023, Plaintiff Wrenn has experienced fraud. On September 3, 2023, the threat actor utilized the Proton electronic mail service to contract Plaintiff Wrenn, threatening to distribute her PII and PHI to her friends, colleagues, and neighbors. Plaintiff Wrenn's image, birthdate, email address and phone number have been also added to the threat actor's leak site(s).

90. In addition, Plaintiff Wrenn's PII and PHI compromised in the Data Breach has been disseminated to her friends, colleagues, neighbors, and others. Plaintiff Wrenn learned of and/or was made aware of the dissemination of her PII and PHI after being told of such dissemination by her friends, colleagues, and neighbors. Plaintiff Wrenn also recently learned of an Instagram account as late as September 8, 2023, which is continuing to disseminate Wrenn's PII and PHI.

91. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Wrenn has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to her friends, colleagues, and neighbors.

92. Since the announcement of the Data Breach, Plaintiff Wrenn has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) in an effort to detect and prevent any misuses of her PII and PHI. Plaintiff Wrenn would not have to undergo such time-consuming efforts but for the Data Breach.

93. As a direct and proximate result of the Data Breach, Plaintiff Wrenn's sensitive PII and PHI has been exposed and Wrenn will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not

speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally used by the threat actor after the Data Breach to extort Plaintiff Wrenn.

Plaintiff Romashova

94. Plaintiff Romashova is a patient of Defendant. On or about March 14, 2023, Plaintiff Romashova received an email notification from Defendant informing her that the PII and PHI she provided to Hankins was compromised in the Data Breach, including her name, Social Security Number, date of birth, and address.

95. Since the announcement of the Data Breach, Plaintiff Romashova has experienced fraud. On July 10, 2023, she received an email from the threat actor stating that they would release her photos and personal information stolen from Hankins. On July 12, 2023, she received another email from the threat actor including a link to a website where nude pre- and post-operation photographs of Plaintiff Romashova and other patients could be found, along with their personal information. Plaintiff Romashova was told by the threat actor that they would remove her information if she paid them $800.

96. When Plaintiff Romashova reached out to Hankins, Defendant told her to submit a claim to the FBI, which she did on July 10, 2023.

97. As a direct and proximate result of Hankins' failure to safeguard her PII and/or PHI, Plaintiff Romashova has been subjected to extortion and the mental anguish of having her sensitive PII and PHI exposed to the public.

98. Since the announcement of the Data Breach, Plaintiff Romashova has been required to spend her valuable time and resources (1) mitigating the risk of the fraud she has experienced and (2) attempting to detect and prevent any misuses of her PII and PHI. Plaintiff Romashova would not have to undergo such time-consuming efforts but for the Data Breach.

99. As a direct and proximate result of the Data Breach, Plaintiff Romashova has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII and PHI compromised in the Data Breach, and that this information was already illegally used by the threat actor after the Data Breach to extort Plaintiff Romashova.

Plaintiffs and Class Members Have Suffered Damages.

100. For the reasons mentioned above, Hankins' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways, including actual fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiffs and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

101. Indeed, the threat actor stole PII and PHI from Hankins with the specific intent to use it for illicit purposes as demonstrated by the threat actor's extortion attempts directed at Plaintiffs and Class Members, along with the sharing of Plaintiffs' and Class Members' PII and PHI with families, friends, and colleagues and posting the same on its leak site(s). These facts distinguish this case from other data breaches that involve only a speculative risk of harm.

102. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Hankins' conduct. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

103. As a result of Hankins' failures, Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

104. With respect to healthcare breaches, another study found "the majority [70 percent] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[29]

105. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[30]

106. Indeed, PII and PHI are valuable commodities to identity thieves and once they have been compromised, criminals will use them and trade the information on the cyber black market for years thereafter. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account routing numbers can fetch up to $1,200 to $1,300 each on the black market.[31] According to a report released by the FBI's cyber division, criminals can sell healthcare records for 50 times the price of stolen Social Security Numbers or credit card numbers.[32]

107. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[33]

108. Health information in particular is likely to be used in detrimental ways, by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[34]

109. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft.

---

[29] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTHITSECURITY, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Sept. 15, 2023).

[30] *Id.*

[31] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Media, (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[32] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[33] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[35]

110. Plaintiffs and Class Members are also at a continued risk because their information remains in Hankins' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Hankins fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

111. Plaintiffs and Class Members have lost the benefit of their bargains. Plaintiffs and Class Members entered into agreements with and provided payment to Hankins under the reasonable but mistaken belief that it would reasonably and adequately protect their PII and PHI. Plaintiffs and Class Members would not have entered into such agreements and would not have paid Hankins the amount that they paid had they known that Hankins would not reasonably and adequately protect their PII and PHI. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the healthcare services that include reasonable and adequate data security that they bargained for, and the healthcare services that do not, which they actually received.

112. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers and their families, friends, and colleagues.

CLASS ACTION ALLEGATIONS

113. Plaintiffs bring this class action on behalf of themselves and all others who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

114. Plaintiffs seek to represent the following Class of persons defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Hankins Data Breach which occurred on or about February 23, 2023 (the "Class").

115. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs,

---

[34] *Id.*

successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

116. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

117. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Hankins' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 12,500 individuals.

118. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Hankins had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Hankins was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Hankins entered contracts implied in fact with Plaintiffs and the Class;

d. Whether Hankins breached those contracts by failing to adequately safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether Hankins was unjust enriched to the detriment of Plaintiffs and the Class;

f. Whether Hankins' conduct is violative of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600;

---

[35] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-

g. Whether Plaintiffs and Class Members are entitled to damages as a result of Hankins' wrongful conduct; and

h. Whether Plaintiffs and Class Members are entitled to restitution as a result of Hankins' wrongful conduct.

119. **Typicality:** Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs' and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and Class Members were all patients of Hankins, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

120. **Adequacy:** Plaintiffs are adequate representatives of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

121. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

122. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

---

id-theft-healthcare.pdf (last visited Sept. 15, 2023).

123. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

124. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Hankins' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiffs on Behalf of Class)

125. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

126. Hankins owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and/or PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiffs' and Class Members' PII and/or PHI in Hankins' possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

127. Hankins' duty to use reasonable care arose from several sources, including but not limited to those described below.

128. Hankins had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII/PHI that is routinely targeted by cyber-criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

129. Hankins' duty also arose from Defendant's special relationship with its patients as a result of its position as a healthcare provider. Hankins holds itself out as a trusted provider of healthcare services, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Hankins who directly provides healthcare services, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

130. Further, Hankins duty arose from various statutes requiring Defendant to implement reasonable data security measures, including but not limited to, Section 5 of the FTC Act, HIPAA, and Nev. Rev. Stat. § 603A.210.

131. Hankins' is subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs and Defendant and Class Members. The sources of Hankins' duty are identified above.

132. Hankins' violation of Section 5 of the FTC Act, HIPAA, and stat data security statutes constitutes negligence *per se* for purposes of establish the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs and Class Members belong and to prevent the type of harm that resulted from the Data Breach.

133. Hankins' conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Hankins conduct included its failure to adequately restrict access to its computer networks that held patients' PII and PHI.

134. Hankins knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII and PHI, and the frequency of cyberattacks such as the Data Breach in the healthcare sector.

135. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII and/or PHI of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and Class Members' PII and/or PHI in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

136. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, their PII and/or PHI would not have been compromised.

137. As a direct and proximate result of Hankins' negligence, Plaintiffs and Class Members have suffered injuries, including: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or

unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

138. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiffs on behalf of the Class)

139. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

140. Plaintiffs bring this claim individually and on behalf of the Class.

141. When Plaintiffs and Class Members provided their PII and PHI to Hankins in exchange for healthcare services, they entered into implied contracts with Defendant, under which Hankins agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII and PHI.

142. Hankins solicited and invited Plaintiffs and Class Members to provide their PII and PHI, including their names, addresses, dates of birth, phone numbers, email addresses, various forms of identification, and medical information, as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Hankins' offers and provided their PII and PHI to Defendant.

143. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Hankins employed adequate data security measures to safeguard their PII and PHI. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide PII and/or PHI, was the latter's obligation to: (a) use such PII and/or PHI for business purposes only, (b) take reasonable steps to safeguard that PII and/or PHI, (c) to prevent unauthorized disclosures of the PII

and/or PHI, (d) to provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and/or PHI, (e) to reasonably safeguard and protect the PII and/or PHI of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) to retain the PII and/or PHI only under conditions that kept such information secure and confidential.

144. Plaintiffs are informed and believe that in Defendant's written privacy policies, Hankins expressly promised Plaintiffs and Class Members that Defendant would only disclose PII and/or PHI under certain circumstances, none of which relate to the Data Breach. Plaintiffs and Class Members paid money to Hankins in the form of co-pays and other similar payments in order to receive healthcare services. Plaintiffs and Class Members reasonably believed and expected that Hankins would use part of those funds to obtain adequate data security. Hankins failed to do so.

145. Plaintiffs and Class Members would not have provided their PII and PHI to Defendant had they known that Hankins would not safeguard their PII and PHI as promised.

146. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Hankins.

147. Hankins breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI.

148. The losses and damages Plaintiffs sustained, include, but are not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

149. As a direct and proximate result of Hankins' breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on Behalf of the Class)

150. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

151. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' Implied Contract claim.

152. Upon information and belief, Hankins funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

153. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Hankins.

154. Plaintiffs and Class Members conferred a monetary benefit on Hankins. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII and/or PHI. In exchange, Plaintiffs and Class Members should have received from Hankins the goods and services that were the subject of the transaction and have their PII and/or PHI protected with adequate data security.

155. Hankins knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Hankins profited from these transactions and used the PII and/or PHI of Plaintiffs and Class Members for business purposes, including very personal photographs taken of Plaintiffs and Class Members.

156. In particular, Hankins enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Hankins instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a

direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

157. Under the principles of equity and good conscience, Hankins should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

158. Hankins failed to secure Plaintiffs' and Class Members' PII and/or PHI and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

159. Hankins acquired the PII and/or PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

160. If Plaintiffs and Class Members knew that Defendant had not secured their PII and/or PHI, they would not have agreed to provide their PII and/or PHI to Hankins, including very personal photographs taken of Plaintiffs and Class Members.

161. Plaintiffs and Class Members have no adequate remedy at law.

162. As a direct and proximate result of Hankins wrongful conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

163. As a direct and proximate result of Hankins' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

164. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services, or Defendant should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

FOURTH CAUSE OF ACTION
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(Plaintiffs on Behalf of the Class)

165. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

166. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part:

167. An action may be brough by any person who is a victim of consumer fraud.

168. As used in this section, "consumer fraud" means: . . . A deceptive trade practice defined in NRS 598.0915 to 598.0225, inclusive.

Nev. Rev. Stat. § 41.600(1) & (2)(e).

169. In turn, Nev. Rev. Stat. § 598.0923(2) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [f]ails to disclose a material fact in connection with the sale or lease of goods or services." *Id.* Hankins violated this provision because it failed to disclose the material fact that its data security measures were inadequate to reasonably safeguard its patients' PII and PHI. This is true because, among other things, Hankins was aware that the healthcare sector is a frequent target of cyberattacks such as the Data Breach. Hankins knew or should have known that that its data security measures were insufficient to guard against attacks such as the Data Breach. Hankins and knowledge of the facts that constituted the omission. Hankins could have and should have made a proper disclosure when accepting new patients, while providing healthcare services, or by any other means reasonably calculated to inform customers of its inadequate data security measures.

170. Further, Nev. Rev. Stat. § 598.0923(3) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal statute or regulation relating to the sale or lease of goods or services." *Id.* Hankins violated this provision for several reasons, each of which serves as an independent basis for violating Nev. Rev. Stat. § 598.0923(3).

171. First, Hankins breached its duty under Nev. Rev. Stat. § 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." *Id.* Hankins is a "data collector" as defined by Nev. Rev. Stat. § 603A.030. Hankins failed to implement such reasonable security measures, as shown by a system-wide breach of its computer systems during which a threat actor exfiltrated patient PII and PHI that was later used to extort Plaintiffs and Class Members. Hankins' violation of this statute was done knowingly for the purposes of Nev. Rev. Stat. § 598.0923(3) because Hankins knew or should have known that the healthcare sector is a frequent target of cyberattacks such as the Data Breach. Hanins knew or should have known that its data security measures were inadequate to protect against cyberattacks such as the Data Breach.

172. Second, Hankins violated Section 5 of the FTC Act and HIPAA, as alleged above. Hankins knew or should have known that its data security measures were inadequate, violated Section 5 of the FTC Act, violated HIPAA, failed to adhere to the FTC's data security guidance, and failed to adhere to HHS's data security guidance. This is true because Hankins was well aware that the healthcare sector is a frequent target of cyberattacks such as the Data Breach and both the FTC and HHS have recommended various data security measures that companies such as Defendant could have implemented to mitigate the risk of a Data Breach. Hankins chose not to follow such guidance and knew or should have known that its data security measures were inadequate to guard against cyberattacks such as the Data Breach. Hankins had knowledge of the facts that constituted the violation. Hankins' violation of Section 5 of the FTC Act and HIPAA serve as a separate actional basis for purposes of violating Nev. Rev. Stat. § 598.0923(3).

173. Hankins engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Class Members.

174. Plaintiff and members of the Class were denied a benefit conferred on them by the Nevada legislature.

175. As a direct and proximate result of the foregoing, Plaintiffs and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

176. As a result of these violations, Plaintiffs and Class Members are entitled to an award of actual damages, equitable injunctive relief requiring Defendant to implement adequate data security measures, as well as an award of reasonable attorney's fees and costs. Nev. Rev. Stat. § 41.600(3).

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

177. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

178. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Consolidated Amended Class Action Complaint.

179. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Hankins is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

180. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Hankins owed a legal duty to secure members' PII and PHI under the common law, Section 5 of the FTC Act, HIPAA, and state data security laws; and

b. Hankins breached and continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

181. This Court also should issue corresponding prospective injunctive relief requiring Hankins to employ adequate security protocols consistent with law and industry standards to protect members' PII and PHI.

182. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Hankins. The risk of another such breach is real, immediate, and substantial. If another breach at Hankins occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

183. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Hankins if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Hankins of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Hankins has a pre-existing legal obligation to employ such measures.

184. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Hankins, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and consumers whose confidential information would be further compromised.

SIXTH CAUSE OF ACTION
NEGLIGENT MISREPRESENTATION
(Plaintiffs on behalf of the Class)

185. Plaintiffs restate and reallege all preceding allegations set forth above as if fully alleged herein.

186. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which imposes liability for negligent misrepresentations based on omissions. Section 551, titled "Liability for Nondisclosure," states:

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if . . . he is under a duty to the other to exercise reasonable care to disclose the matter in question.

187. As a healthcare provider, and a recipient of its patients' PII and PHI, Defendant has a special relationship with its patients, including Plaintiffs and members of the Class.

188. Because of that special relationship, Hankins was provided with and stored private and valuable PII and PHI related to Plaintiffs and the Class. Plaintiffs and Class Members were entitled to expect that the PII and PHI entrusted to Hankins would remain confidential while in Hankins' possession.

189. Despite this special relationship, Hankins failed to disclose to Plaintiffs and Class Members that it did not employ reasonable data security safeguards to protect patients' PII and PHI.

190. Hankins's omissions were made for the guidance of patients in their transactions with Hankins.

191. Hankins failed to disclose facts that Hankins knew may justifiably induce patients to act or refrain from acting in their decision to engage with Hankins to provide them with healthcare services.

192. Hankins' omissions were made in the course of Hankin' provision of healthcare services to Plaintiffs and Class members.

193. Hankins had a duty to speak regarding the inadequacy of its data security practices and its inability to reasonably protect patients' PII and PHI.

194. Hankins knew or should have known that its data security practices were deficient. This is true because, among other things, Hankins was aware that the healthcare industry was a frequent target of sophisticated cyberattacks. Hankins knew or should have known that its data security practices were insufficient to guard against those attacks.

195. Hankins was in a special relationship with, or relationship of trust and confidence relative to, its patients. Hankins was in an exclusive position to ensure that its safeguards were sufficient to protect against the foreseeable risk that a data breach could occur. Hankins was also in exclusive possession of the knowledge that its data security processes and procedures were inadequate to safeguard patients' PII and PHI.

196. Hankins' omissions were material given the sensitivity of the PII and PHI maintained by Hankins and the gravity of the harm that could result from theft of the PII and PHI.

197. Data security was an important part of the substance of the transactions between Hankins and its patients.

198. Hankins knew or should have known that patients would enter into the provision of healthcare services under a mistake as to facts basic to the transactions. Because of the relationship between the parties, patients would reasonably expect a disclosure of the basic facts regarding Hankins' inadequate data security.

199. Had Hankins disclosed to Plaintiffs and Class Members that its systems were not secure and thus were vulnerable to attack, Plaintiffs and Class Members would not have entrusted their PII and PHI to Hankins.

200. Hankins should have made a proper disclosure to patients when accepting patient information, during the initial consultant, or by any other means reasonably calculated to inform patients of its inadequate data security.

201. In addition to its omissions, Hankins is also liable for its implied misrepresentations. Hankins required patients to provide their PII and/or PHI during the appointment, consultation and/or check-in process. In doing so, Hankins made implied or implicit representations that it employed reasonable data security practices to protect patients' PII and PHI. By virtue of accepting Plaintiffs' and Class Members' PII and/or PHI during the appointment, consultation and/or check-in process, Hankins implicitly represented that its data security processes were sufficient to reasonably safeguard the PII and/or PHI patients entrusted to Defendant. This constituted a negligent misrepresentation.

202. Hankins failed to exercise reasonable care or competence in communicating its omissions and misrepresentations.

203. As a direct and proximate result of Hankins' omissions and misrepresentations, Plaintiffs and Class Members suffered the various types of damages alleged herein.

204. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiffs demand a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

1. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

2. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

3. For compensatory damages on behalf of Plaintiffs and the Class;

4. For punitive damages on behalf of Plaintiffs and the Class;

5. For an order of restitution and all other forms of equitable monetary relief;

6. Declaratory and injunctive relief as described herein;

7. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

8. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

9. Awarding pre- and post-judgment interest on any amounts awarded;

10. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

11. Awarding such other and further relief as may be just and proper.

Dated this 15th day of September, 2023.

THE BOURASSA LAW GROUP

/s/ Jennifer A. Fornetti
MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102

NICHOLAS A. COLELLA (*pro hac vice*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

RAINA BORRELLI (*pro hac vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com

RAMZY P. LADAH
LADAH LAW FIRM
517 S. Third Street
Las Vegas, NV 89101
Telephone: (702) 252-0055
Facsimile: (702) 248-0055

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

Pursuant to FRCP 5(b), I certify that I am an employee of The Bourassa Law Group, and that on this date I caused to be served a true copy of **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** on all parties to this action by the method(s) indicated below:

X by using the Court's CM/ECF Electronic Notification System addressed to:

Gary E. Schnitzer, Esq.
L. Renee Green, Esq.
Marta D. Kurshumova, Esq.
KRAVITZ SCHNITZER JOHNSON & WATSON, CTD.
Email: gschnitzer@ksjattorneys.com
rgreen@ksjattorneys.com
mkurshumova@ksjattorneys.com

Attorneys for Defendants

DATED: This 15th day of September, 2023.

/s/ Valerie Gray
Employee of The Bourassa Law Group